Introduction

This Services Guide contains provisions that define, clarify, and govern the services described in the quote that has been provided to you (the "Quote"). If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by GRIT Technologies ("GRIT Technologies," "we," "us," or "our"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). Activities or items that are not specifically described in the Quote will be out of scope and are not included unless otherwise agreed to by us in writing.

This Services Guide, along with our Master Services Agreement (located at https://www.grittechs.com/master-services-agreement/ the "MSA") contains important provisions pertaining to the auto-renewal of the Services in the Quote, as well as fee increases that may occur from time-to-time. Please read the MSA, your Quote, and this Services Guide carefully, and keep copies of those documents for your records.

Transition Plan

All of our managed service projects begin with a transition plan. The following table is a high-level overview of the transition plan we will follow, starting with our initial compliance check of your managed IT infrastructure.

Transition Phase	Objectives
Agreement	• Set expectations • Validate objectives • Vision and scope confirmed • Identify key network elements to be monitored • Gather data on IT objectives and plans
Signing of Quote	• CLIENT and GRIT Technologies agree on supported elements and start date
Compliance Check[1]	• Document key network elements • Identify compliant and non-compliant systems • Review compliant and non-compliant systems and devise plan for compliancy
Implement and Compliance[2]	• GRIT Technologies implements monitoring • CLIENT Works in partnership with GRIT Technologies to meet compliancy goals • End user education and contact numbers assigned • Document final setup and configuration • Validate complete system operational before go-live date
Go Live	• Review progress on compliance items • Go live
Ongoing Monitoring	• CLIENT formally accepts project completion • Outcomes measured against project objectives • Administrative close

[1]If deficiencies are discovered during the Compliance Check (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, we cannot guarantee that all Issues will be detected during the Compliance Check process. Issues that are discovered in the managed environment after the Compliance Check process is completed may be addressed in one or more subsequent quotes.

[2] The duration of the implementation process depends on many factors, many of which may be outside of our control—such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the implementation process. We will keep you updated as the implementation process progresses.

Site Infrastructure Service

This section provides details about the services provided by GRIT Technologies relating to office locations and their corresponding network equipment. One location is included in the Services; additional locations may be added by mutual agreement. Each separate office site is billed as an additional location.

- **Internet Router Management –** GRIT Technologies will liaise with your ISP to troubleshoot data issues and configure your network for optimal performance. GRIT Technologies will also open trouble tickets with your ISP and work to get outages resolved. We will assist you with communications with your hosting provider to help facilitate hosting-related issues.
- **Firewall/VPN Management –** GRIT Technologies will actively manage your firewall, monitor security trends, and make sure you stay current with all updates and patches. We will manage your existing VPN through which you remotely access your network. GRIT Technologies will also manage and support your existing firewall services.
- **Managed Switch –** GRIT Technologies will ensure your Ethernet switches are configured properly to optimize network performance and help ensure that critical business systems run properly.
- **Wireless Access Points -** GRIT Technologies will ensure your Wireless Access Points are configured properly to optimize WIFI coverage.
- **Unlimited Technical Support –** When required GRIT Technologies will dispatch a technician to solve issues remotely or over the phone free of charge.

Basic Security End-User Support

This section provides details about Services provided by GRIT Technologies related to each supported employee.

- **Unlimited Helpdesk Support -** Help desk is available during our normal business hours.
    - **Unlimited Support Incidents**

      GRIT Technologies will attempt to fix all issues remotely before coming on site. To establish remote support, the user will be required to allow our technician access to his/her system remotely. Instructions will be given over the phone during the support call.
    - **Microsoft Application Support**

      GRIT Technologies will support most of Microsoft's desktop products. GRIT Technologies has technical staff familiar with Microsoft 365, Microsoft SQL Server, , IIS and many of Microsoft's Server products. We provide timely phone support and technical assistance.
- **Email Protection**
    - Anti-Virus, Anti-Spam, Anti-Malware
    - Allow Lists (Whitelisting)

- Block Lists (Blacklisting)

- **User Account Administration**

  GRIT Technologies will handle add/remove/change requests through its helpdesk service.

- **Ticket Management**

  GRIT Technologies provides each authorized user access to our online ticket management system through Desk Director, allowing visibility into the current status of helpdesk requests. Resolution notes on each incident create a customized knowledge base accessible by your system administrators and end users.

- **Cybersecurity Awareness Program**

  - **Cybersecurity Training**

    Our Cybersecurity Awareness provides participants with online, on-demand information they need to know to help identify the signs of common cybersecurity attacks, as well as how to keep their business credentials secure thereby reducing the risk of a successful cybersecurity attack.

  - **Monthly Simulated Fishing E-Mails**

    To keep skills sharp, GRIT Technologies will send simulated phishing e-mails to each enrolled participant to test his/her cybersecurity awareness skills.

  - **Ongoing Training**

    "Frequent clickers" will be automatically enrolled for refresher training and set up quarterly or semi-annual refresher training for all employees.

  - **Quarterly Reports**

    Quarterly reports of all cybersecurity activity training activity will be provided on a quarterly basis to determine training effectiveness.

- **Dark Web Monitoring**

  - **Detect Stolen or Compromised Credentials**

    With over 2 billion e-mail account credentials for sale on the dark web, there is an active market for buyers and sellers. GRIT Technologies will monitor the dark web for your domain's digital credentials and alert you when they're detected.

  - **Reduce Risk of a Data Breach**

    Dark web monitoring reduces the amount of time between a data breach occurrence and when you're alerted. This shrinks the window of opportunity criminals have to make copies of your data and sell it. Although the credentials can't be removed from the dark web, steps can be taken to render those stolen credentials useless.

- **3rd Party Application Support**

  - **Vendor Account Management -** We understand your company relies on many external technology vendors and software programs to keep your business running. Often with the

interaction of vendor software and your systems it is difficult to troubleshoot and understand where issues and problems originate. GRIT Technologies will facilitate your technology vendor relations. Our expert IT staff can work with any IT vendor with whom you maintain a then-current service or support agreement to troubleshoot your applications or equipment (such as printers or licensed software).

- **Change Request Management -** GRIT Technologies will handle all basic change request management for your vendor software. We will follow vendor-supplied instructions for adding/removing accounts, password resets, permissions troubleshooting and licensing issues.
- **Configuration Review -** GRIT Technologies will evaluate your current vendor software configuration, including backup and recovery, security, and performance. Where needed we will work with the vendor and recommend changes to boost performance and availability.
- **Software Patch Management -** GRIT Technologies will work with your software vendor to help ensure that your critical applications remain updated with the latest required service packs and recommended patches.
- **Performance Monitoring -** We will constantly monitor performance and alert you to performance bottlenecks and work with the applicable vendor(s) to recommend actions to fix performance issues.

Basic Endpoint Toolset

This section provides details about Services provided by GRIT Technologies relating to servers, desktops and laptops.

- **Software Patch Management (Server / Desktop / Laptop) –** Each month, GRIT Technologies will install Microsoft Critical operating system patches on your managed systems to help protect your information. Our patch management service covers:
  - Desktops: Microsoft operating system, Microsoft Office and designated critical Line of Business applications
  - Servers: Microsoft Operating system, IIS, SQL and designated critical applications.
  - Network Devices: Vendor specific patches.
  - GRIT Technologies will provide service pack upgrades within 3 months of the service pack release, and critical security patches within 3 weeks of release.
- **Antivirus, Content filtering, and Software License and Monitoring (Server / Desktop / Laptop) -** Includes providing an antivirus software license along with maintaining a current version on all covered equipment.
- **Virus and Malware Removal**

GRIT Technologies will use its best efforts to remotely remove viruses or other malware that evade the antivirus systems. Please note: Not all viruses and malware can be quarantined or removed. On a case-by-case basis, we will escalate the issue to our third party solution providers for diagnosis and possible remediation.

- **Server and Desktop Optimization and Management (Server / Desktop / Laptop) -** GRIT Technologies will monitor servers 24/7 through our systems management software and schedule daily, weekly, monthly and quarterly server tune-ups to keep your system healthy. Desktop and laptop tune-ups will be completed as necessary. These processes are scheduled during off hours or idle time so as to minimize the impact on your business operations.
- **Asset Management (Server / Desktop / Laptop) -** GRIT Technologies provides historical and daily, real-time view on all asset information on covered assets. This includes real time reporting on installed software to help ensure your business complies with licensing requirements.
- **Monitoring (Server / Desktop / Laptop) -** GRIT Technologies monitors system drive space, CPU, memory, and key Windows services and alerts Client to critical events. This service is also an essential aid to assisting Client with long term capacity-related planning.

Helpdesk Policies

This section covers GRIT Technologies' policies for helpdesk services.

- **Helpdesk Contact Methods**

  GRIT Technologies will accept helpdesk requests via email, phone, voicemail or the client portal. GRIT Technologies can be reached at 586-286-8324, emailed at support@grittechs.com.com, or via the end user portal at www.grittechs.com.

- **Helpdesk Hours of Operation**

  Clients have normal access to helpdesk during normal working hours 7AM through 5PM EST Monday through Friday, excluding GRIT Technologies Holidays: New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, day after Thanksgiving, and Christmas Day.

- **Service Levels, Issue Priority and Response Time**

  Automated monitoring is provided on an ongoing (i.e., 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our normal business hours unless otherwise specifically stated in the Quote.

  We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined our discretion after consulting with the Client. All remediation services will initially be attempted remotely; we will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

	High Urgency	Medium Urgency	Low Urgency
High Impact	Priority 1	Priority 2	Priority 2
Medium Impact	Priority 2	Priority 3	Priority 3
Low Impact	Priority 3	Priority 3	Priority 4

Urgency

High – Whole company is affected
Medium – Departments or large group of users are affected
Low - One user or a small group of users is affected

Impact

High – Critical! Major business processes are stopped
Medium – Business is degraded, but there is a reasonable workaround
Low – More of an irritation than a stoppage

Response time

	Respond Within	Resolution Plan Within	Goal %
Priority 1 - Emergency Response	0.2 Hours	1 Hour	>90
Priority 2 - Quick Response	0.2 Hours	4 Hours	>90
Priority 3 - Normal Response	0.2 Hours	24 Hours	>90
Priority 4 - Low Response	0.2 Hours	168 Hours	>90

SLA Clocks run Monday through Friday from 7 AM to 5 PM.

After hours, support can be obtained by calling our service desk. If not answered right away, the on-call engineer will call back within 2 hours. Between 9 PM and 5:30 AM, all calls will go to VM. At 5:30 AM if there are any VMs or alerts, the on-call engineer will be alerted and address the issue.

- **Reporting**

  GRIT Technologies will provide regular activity reports detailing helpdesk activity, call volumes and usage. Ad hoc reports are available as requested. Reports will be provided via email to the primary client contact or through a business.

- **Hardware and Software Policies**
  - GRIT Technologies plans do not include hardware replacement for covered items. Any parts needed will be quoted for Client approval.
  - GRIT Technologies must be made aware of any changes to server, desktop and network hardware that will affect support calls and maintainability in writing 5 days before the change. A change in number of devices covered under GRIT Technologies' maintenance and support will be reflected accordingly in the monthly rates.
  - Hardware and application software must be supported and properly licensed at all times. Hardware or software that falls out of support or fails to meet vendor licensing will not be supported.
  - These Services are intended to MAINTAIN the EXISTING system. Installing anything new into the managed environment is out of scope. Service packs and patches are considered maintaining the managed environment. Version upgrades, if provided, are considered to be project related and billed separately.

- **Service Credits**

  Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing

(within 90 days after the applicable failure), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Quote.

System Compliance – Minimum Requirements

To ensure the efficiency and effectiveness of our services, we require that your managed devices meet or exceed certain minimum compliancy requirements. Initially, we will look at all of your devices and designate those devices as "compliant," "semi-compliant, or "non-compliant"—see below for more details.

- **Compliance Levels**
  - **Compliance Categories**

    Network devices including servers, desktops, and network components will fall into one of three categories: Compliant, Semi-compliant or Non-compliant. **GRIT Technologies bases its support pricing on servicing compliant systems. Semi-compliant or non-compliant systems will incur an additional charge.**

  - **Keeping Systems in Compliance**

    Network devices will be evaluated on a periodic basis and if managed devices and/or the managed environment fall into a higher charge category, Client will have 30 days to bring the applicable device(s) back into compliance. Devices or environments that move from non-compliant or semi-compliant to compliant will revert to standard pricing 30 days after the move to compliancy.

- **Network and Endpoint Compliance Check**

  GRIT Technologies will schedule network compliance checks to determine the health and compliance level of managed equipment. GRIT Technologies will provide Client with a report outlining Client's key network elements and their compliancy levels.

  Minimum Requirements: The following minimum requirements must be maintained at all times by Client:

  - All licensing must be up to date; active support agreements must be in place for critical software.
  - All desktops and servers must meet software vendor minimum recommended processor speed, memory, and available hard drive space.
  - All desktops, servers and network devices and software must be at the vendor recommended service pack and patch level.
  - All hardware must be within warranty or replacement systems available during the life of the contract.

- A managed Meraki Firewall or equivalent appliance with an active support subscription in place for each location.
- Regularly scheduled offsite backup rotations are completed for servers and critical data and MUST use Imaging Technology allowing for full image restore.
- Hot-swap disks available for servers in case of drive failure.
- All servers, desktops and network devices have current antivirus (as applicable) and must be free of viruses and spyware/adware at the commencement of the service contract.
- All servers connected to an uninterruptible power supply, such as APC.
- Network switches must be vendor-supported, stackable and managed switches with Gigabit speed capability, such as Meraki or Unifi.
- All endpoints must be connected to a gigabit switch via a single, uninterrupted CAT5 or better cable.
- Business-class internet service required
- The network must be secure with a best practices security audit conducted.
- Wireless access points should be vendor-supported and business-class, such as Meraki or Unifi.

GRIT Technologies reserves the right to refuse to cover a device or software based on the initial network assessment. Client will have a grace period of 30 days to get their systems to the agreed to compliancy level, thereafter GRIT Technologies has the option of increasing the rate on non-compliant systems as described in the following table:

Compliancy Level	**Compliancy Level Description**	**Additional Charges**
Compliant	No more than one item in violation on compliance checklist	None
Semi-Compliant	No more than two items in violation on compliance checklist	25% additional support cost for each semi-compliant system
Non-Compliant	Does not meet three or more items from compliancy checklist	50% additional support cost for each non-compliant system

Fees

The fees for the Services will be as indicated in the Quote.

Changes to managed environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the

managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

Minimum Monthly Fees. The initial Fees indicated in Quote are the minimum monthly fees ("MMF") that will be charged to you during the term. You agree that the amounts paid by you under the Quote will not drop below the MMF regardless of the number of users or devices to which the Services are directed or applied, unless we agree to the reduction. All modifications to the amount of hardware, devices, or authorized users under the Quote (as applicable) must be in writing and accepted by both parties.

Increases. In addition, we reserve the right to increase our monthly recurring fees and, if applicable, our data recovery-related fees; provided, **however, if an increase is more than fifteen percent (15%) of the fees charged for the Services in the prior calendar year**, then you will be provided with a sixty (60) day opportunity to terminate the Services by providing us with written notice of termination. You will be responsible for the payment of all fees that accrue up to the termination date and all pre-approved, non-mitigatable expenses that we incurred in our provision of the Services through the date of termination. Your continued acceptance or use of the Services after this sixty (60) day period will indicate your acceptance of the increased fees.

In addition to the foregoing, we reserve the right to pass through to you any increases in the costs and/or fees charged by third party providers for the third party services ("Pass Through Increases"). Since we do not control third party providers, we cannot predict whether such price increases will occur, however, should they occur, we will endeavor to provide you with as much advance notice as reasonably possible.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

Automated Payment. You may pay your invoices by credit card and/or by ACH, as described below. If you authorize payment by credit card and ACH, then the ACH payment method will be attempted first. If that attempt fails for any reason, then we will process payment using your designated credit card.

- **ACH**. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.
- **Credit Card**. When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote. We reserve the right to charge a convenience fee on all credit card transactions which will be the greater of 3.2% of the amount being charged, or the cost that we are charged by our merchant bank to accept your card.

- **Check.** You may pay by check provided that your check is delivered to us prior to the commencement of Services. Checks that are returned to us as incorrect, incomplete, or "not sufficient funds" will be subject to a $50 administration fee and any applicable fees charged to us by your bank or financial institution.

Microsoft Licensing Fees. The Services require that we purchase certain "per seat" licenses from Microsoft (which Microsoft refers to as New Commerce Experience or "NCE Licenses") in order to provide you with one or more of the following applications: Microsoft 365, Dynamics 365, Windows 365, and Microsoft Power Platform (each, an "NCE Application"). To leverage the discounts offered by Microsoft for these applications and to pass those discounts through to you, we will purchase NCE Licenses for one (1) year terms for the NCE Applications required under the Quote. **As per Microsoft's requirements, NCE Licenses cannot be canceled once they are purchased and cannot be transferred to any other customer. Each NCE License that we purchase may require a one (1) or three (3) year term. For that reason, you understand and agree that regardless of the reason for termination of the Services, you are required to pay for all applicable NCE Licenses in full for the entire term of those licenses.** Provided that you have paid for the NCE Licenses in full, you will be permitted to use those licenses until they expire, even if you move to a different managed service provider.

Additional Terms

Remediation

Unless otherwise expressly provided in the Quote, remediation services will be provided in accordance with the recommended practices of the managed services industry. Client understands and agrees that remediation services are not intended to be, and will not be, a warranty or guarantee of the functionality of the managed environment, or a service plan for the repair of any particular piece of managed hardware or software.

Configuration of Third Party Services

Certain third party services provided to you under this Services Guide may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without our knowledge or authorization could disrupt the Services and/or or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

Modification of managed environment

Changes made to the managed environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the managed environment without our prior knowledge or consent. For example, you agree to refrain from adding to or removing hardware from the managed environment, installing applications in the

managed environment, or modifying the configuration or log files of the managed environment without our prior knowledge or consent.

Co-Managed managed environment

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by us), we will endeavor to implement the Services in an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the managed environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist in the managed environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. To improve security awareness, you agree that GRIT Technologies or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data impacted by the incident will be recoverable. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the managed environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all Services described or designated as "unlimited" or that do not have a "fixed" or "capped" amount of time allocated to them. You may use those Services as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our

technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from:

- Creating urgent support tickets for non-urgent or non-critical issues;
- Requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training); or,
- Requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

In addition, you agree to replace chronically failing or obsolete equipment that negatively impacts the managed environment or that requires us to commit, in our determination, an inordinate amount of time or effort to remediate.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email"). Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by GRIT Technologies or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. GRIT Technologies reserves the right, but not the obligation, to suspend Client's access to the Hosted Email and/or all transactions occurring under Client's Hosted Email account(s) if GRIT Technologies believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Patch Management

Patches are developed by third party vendors and, on rare occasions, may make the managed environment, or portions of the managed environment, unstable or cause the managed equipment or software to fail to function properly even when the patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any patch. We reserve the right, but not the obligation, to refrain from installing a patch if we are aware of technical problems caused by a patch, or we believe that a patch may render the managed environment, or any portion of the managed environment, unstable.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither GRIT Technologies nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. GRIT Technologies cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that GRIT Technologies shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a local backup of all of stored data to mitigate against the unintentional loss of data.**

Procurement

Equipment and software procured by GRIT Technologies on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, GRIT Technologies does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Client's responsibility if a return of the Procured Equipment is requested. GRIT Technologies is not a warranty service or repair center. GRIT Technologies will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which GRIT Technologies will be held harmless, and (ii) GRIT Technologies is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Business Review / IT Strategic Planning Meetings

We strongly suggest that you participate in business review/strategic planning meetings as may requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

VCTO or VCIO Services

The advice and suggestions provided us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. GRIT Technologies will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary realtionship with Client. Under no circumstances shall Client list or place the GRIT Technologies on Client's corporate records or accounts.

Sample Policies, Procedures.

From time to time, we may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to

be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity are not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

Obsolescence

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires "end of support" status from the applicable device's or software's manufacturer ("Obsolete Element"), then we may designate the device or software as "unsupported" or "non-standard" and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our "best efforts" only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element, or (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose). In any event, we make no representation or warranty whatsoever regarding any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

Licenses

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.